

Reply to the First Office Action

CLAIMS

What is claimed is:

1. A method for verifiably transmitting an electronic package from a sender to a recipient through a certifying authority via a public communications network, the method comprising the steps of:

- the sender logging on to a certifying authority using a standard authentication protocol;
- the certifying authority creating an electronic package from inputs transmitted by the sender via the public communications network;
- the certifying authority storing the inputs relating to the electronic package on a server operated by the certifying authority for use in later verifying the inputs relating to the electronic package and storing any other data received from the sender;
- delivering a message relative to the electronic package from the certifying authority to the recipient via the public communications network;
- the recipient logging on to the certifying authority as a response to the receipt of the message;
- the certifying authority generating an encrypted hash value based on the inputs relating to the electronic package and the delivery thereof, the encrypted hash value uniquely identifying the particulars relating to the electronic package and the delivery thereof; and

Reply to the First Office Action

- transmitting an electronic certificate of service from the certifying authority via the public communications network, the electronic certificate of service including selected inputs relating to the electronic package and a digital certificate

2. The method of claim 1 further comprising the steps of:

- storing the electronic package inputs and other related data on the server operated by the certifying authority for use in later producing a duplicate of the electronic package for a period of time agreed upon by the certifying authority and the sender; and

- storing the inputs comprising: the name and address of the email sender, the name and address of the recipient, the name and email of the address of any other persons to whom the certificate of service has been delivered, the time of delivery, the date of delivery, the subject of the message, the size of the message, the electronic package retention expiration date, the name of each attachment, and the size of each attachment.

3. The method of claim 1 wherein the certifying authority embeds the digital certificate on the face of the electronic certificate of service.

Reply to the First Office Action

4. The method of claim 1 wherein the certifying authority embeds the digital certificate in the electronic certificate of service electronically.
5. The method of claim 1 wherein a recipient, sender or other person requests the certifying authority to employ the digital certificate embedded within the electronic certificate of service so as to verify that the contents of the electronic package stored on the certifying authority's server are identical to the description thereof found on the face of the electronic certificate of service.
6. The method of claim 1 wherein the certifying authority utilizes the embedded digital certificate within the electronic certificate of service to locate and identify the electronic package.
7. The method of claim 1 wherein the certifying authority, having located and identified the electronic package, reproduces the electronic package identically to that first assembled by the certifying authority.
8. The method of claim 1 wherein the reproduced electronic package is certified to be a true and correct copy of the original electronic package, such certification being made by the certifying authority.

Reply to the First Office Action

9. The method of claim 1 wherein the certifying authority issues a certification to a requesting party that the reproduced electronic package is a true and correct copy of the original electronic package and said certification and electronic package are delivered to said requesting party.

10. The method of claim 1 wherein the particulars surrounding the electronic package comprises a maximum number of days within which to deliver the electronic package to the recipient.

11. The method of claim 10 further comprising the step of informing the sender, in event that delivery was not made to the recipient within the maximum number of days, by delivering to the sender and other appropriate persons, an electronic certificate of non-service.

12. The method of claim 1 wherein the particulars surrounding the electronic package comprises a date through which the electronic package is to be stored by the certifying authority.

13. The method of claim 1 wherein tracked message includes an email message and an email attachment and wherein the particulars surrounding the electronic package comprises identity of sender, email address of sender, identity of recipient, email address of recipient, date of transmission, time of

Reply to the First Office Action

transmission, length of the email message, name of the email attachment, and size of the email attachment.

14. The method of claim 1 further comprising the steps of creating the electronic certificate of service as an encrypted file.

15. The method of claim 1 wherein the step of creating the electronic certificate of service as an encrypted file is accomplished by creating an encrypted PDF file that is printable but not modifiable.

16. The method of claim 1 further comprising the step of verifying an encrypted hash value that is questioned by transmitting the encrypted hash value to the certifying authority; and comparing the encrypted hash value that is questioned with records of the certifying authority.

17. The method of claim 1 further comprising the step of notifying the recipient via the public communications network that the electronic package is available for pickup from the server operated by the certifying authority

18. The method of claim 16 wherein the step of delivering the electronic package from the certifying authority to the recipient via the public communications network occurs upon a request for download thereof by the

Reply to the First Office Action

recipient; and wherein the step of transmitting an electronic certificate of service from the certifying authority via the public communications network takes place after completion of the delivering step.

19. The method of claim 1 wherein particulars of the inputs of the recipient that are converted to an electronic package by the certifying authority are encrypted using an encrypted key maintained solely by the certifying authority for the purpose of embedding the same into the electronic certificate of service.

20. The method of claim 1 wherein the step of transmitting an electronic certificate of service transmits an electronic certificate of service to the sender.

21. The method of claim 1 wherein the step of transmitting an electronic certificate of service transmits an electronic certificate of service to the recipient.

22. The method of claim 1 wherein the step of transmitting an electronic certificate of service transmits an electronic certificate of service to a designee of the sender other than the recipient.